Remarks

1. Claims 1-21 are pending.

2. The objection to claims 1, 3, 6-8,12, 18 and 20 has been withdrawn in light of the amendments to the claims in the last response and the previous rejection of claims 1-7, 18 and 19 under 35 USC § 112 (second paragraph) has been withdrawn.

3. Claims 8 and 20 stand rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. Claims 1-21 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Halasz et al. (US Patent No. 6,996,714) in view of Mackenzie (US Publication No. 2002/0194478) further in view of Chen et al. (US Patent No. 5,784,463).

5. Claims 1, 3, 5, 6, 7, 8, 15, 18 and 20 have been amended. No new matter has been added.

Support for the amendments to claims 1, 8, 15, 18 and 20 may be found at least in original claim 3 and page 7 lines 2-4 of PCT/KR2004/001569.

6. Rejections under 35 U.S.C. 112

Claims 8 and 20 stand rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 8 and 20 have been amended to make clear that the encrypted value "the encrypted value" is referring back to encrypted value of the step c, which is generated by the subscriber station and received by the authentication server.

Applicant submits that the Examiner's rejection under 35 U.S.C. 112 is now moot.

7. Rejections under 35 U.S.C. 103(a)

Claims 1-21 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Halasz et al. (US Patent No. 6,996,714) in view of Mackenzie (US Publication No. 2002/0194478) further in view of Chen et al. (US Patent No. 5,784,463).

Claims 1, 8, 15, 18 and 20 are independent claims.

In the Office Action the Examiner states:

"As per claim 1 and 18,

Halasz teaches in a key exchange method for mutual authentication at a subscriber station accessed to an authentication server through a wired/wireless communication, a two-factor authenticated key exchange method comprising: the subscriber station receiving a random number generated by the authentication server; encrypting a first predetermined value using the received random number, a password predefined in the subscriber station, and a key stored in a token, and transmitting the encrypted first predetermined value and a generated authenticator of the subscriber to the authentication server (column 7, lines 7-50); the subscriber station receiving the authentication server's authenticator from the authentication server (column 7, lines57-column 8, line 15).

Halasz does not explicitly teach the subscriber station transmitting a key to the authentication server, the key being generated using an identifier of the subscriber station and a public key of the authentication server; authenticating the generated authenticator of the subscriber using the encrypted first predetermined value and generates the authentication server's authenticator when the authentication is successful; and wherein the authentication server's authenticator is generated by the authentication server using the encrypted first predetermined value transmitted from the subscriber station, and wherein the subscriber station authenticates the authentication server's authenticator using the first predetermined value. However, in an analogous art, Mackenzie teaches the subscriber station transmitting a key to the authentication server, the key being generated using an identifier of the subscriber station and a public key of the authentication server (paragraph [0060], [0062]). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Halasz to include the subscriber station transmitting a key to the authentication server, the key being generated using an identifier of the subscriber station and a public key of the authentication server. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to improve computational efficiency associated with network authentication and key exchange (paragraph [0002]). Halasz in view of Mackenzie does not explicitly teach; authenticating the generated authenticator of the subscriber using the encrypted first predetermined value and generates the authentication server's authenticator when the authentication is successful; and wherein the authentication server's

authenticator is generated by the authentication server using the encrypted first predetermined value transmitted from the subscriber station, and wherein the subscriber station authenticates the authentication server's authenticator using the first predetermined value. However, in an analogous art, Chen teaches authenticating the generated authenticator of the subscriber using the encrypted first predetermined value (column 5, lines 48-54) and generates the authentication server's authenticator when the authentication is successful (column 5, lines 54-60); and wherein the authentication server's authenticator is generated by the authentication server using the encrypted first predetermined value transmitted from the subscriber station, and wherein the subscriber station authenticates the authentication server's authenticator using the first predetermined value (column 5, lines 58-62).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Halasz and Mackenzie to include authenticating the generated authenticator of the subscriber using the encrypted first predetermined value and generates the authentication server's authenticator when the authentication is successful; and wherein the authentication server's authenticator is generated by the authentication server using the encrypted first predetermined value transmitted from the subscriber station, and wherein the subscriber station authenticates the authentication server's authenticator using the first predetermined value. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to secure a computer system from unauthorized access over an open or public network to which the computer is connected (column 1, lines 9-11)."

The Examiner makes similar statements with regard to independent claims 8, 15 and 20.

Applicant has reviewed the Halasz, Mackensie and Chen references with care, paying particular attention to the passages cited, and submits that claims 1, 8, 15, 18 and 20 as amended are not obvious in view of these references.

Applicant submits that neither Halasz, Mackensie and Chen teach or suggest "*the subscriber station generating a random number and precomputing a first predetermined value when the subscriber station does not exchange a key for authentication with the authentication server*", as recited in claim 1 and similarly in claims 8, 15, 18 and 20. (emphasis added)

Further, Applicant submits that Halasz, Mackensie and Chen teach away from the above feature.

Halasz in col. 7 lines 35 to 60, shown below, teaches that the client 106 and the authentication server 110 exchange key information, which teaches away from "*the subscriber*

station generating a random number and precomputing a first predetermined value when the subscriber station does not exchange a key for authentication with the authentication server", as recited in claim 1 and similarly in claims 8, 15, 18 and 20. (emphasis added)

"Referring now to FIG. 3, there is illustrated a general flow chart of the protocol process for mutual authentication between the wireless client 106 and AS 110 of FIG. 1a. Flow begins at a Start terminal and moves to a function block 300 where the client 106 associates to the AP 102. The AP 102 then sends an EAP identity request to the client 106, as indicated in a function block 302. Flow is to a function block 304 where the username and password of the client user are obtained (e.g., via a login process) in the client 106. The username is transmitted from the client 106 to the AP 102, and forwarded from the AP 102 to the AS 110. The AS 110 then issues a challenge to the client 106, as indicated in a function block 306. *In a function block 308, the client 106 responds by performing a DES encryption step, and sending the DES encrypted data to the AS 110. The AS 110 does the same DES encryption based on information corresponding to the received username and checks it against the encrypted response data received from the client 106*. Flow is then to a decision block 312 where if the client 106 is not a valid client, flow is out the "N" path to a function block 314 to deny network access to the client 106. Flow then loops back to the input of function block 300 to reinitiate the association process. If the AS 110 determines that the client is valid, flow is out the "Y" path of decision block 312 where the AS 110 notifies the AP 102 that the client is valid, which AP 102 forwards the validation information to the client 106." (emphasis added)

Similarly, MacKensie in paragraph [0030], shown below, teaches that a client and an authentication server exchange information to compute a shared secret key, which teaches away from "*the subscriber station generating a random number and precomputing a first predetermined value when the subscriber station does not exchange a key for authentication with the authentication server*", as recited in claim 1 and similarly in claims 8, 15, 18 and 20. (emphasis added)

"[0030] A key exchange protocol called Diffie-Hellman Key Exchange and described in W. Diffie and M. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, vol. 22, no. 6, 644-654, 1976, the disclosure of which is incorporated by reference herein, is based on the modular exponentiation function. Specifically, two parties A and B agree on a secret key in accordance with the protocol described in conjunction with FIG. 1. In step 102, A chooses a random x from the group Z.sub.q (i.e., x .epsilon..sub.R Z.sub.q) where Z.sub.q={0, 1, . . . , q-1} (or simply the integers mod q). In step 104, A computes X=g.sup.x mod p. In step 106, A transmits X to B. In step 108, B chooses a random y from Z.sub.q (i.e., Y .epsilon..sub.R Z.sub.q) In step 110, B computes Y=g.sup.y mod p and *transmits Y to A in step 112*. At this point, a shared secret g.sup.xy (i.e., a secret key) can be computed by both A and B. Note that

herein below we may ignore the mod p notation for notational simplicity if it is clear that we are working in mod p. *Since X=g.sup.x was transmitted from A to B in step 106, B can calculate the shared secret g.sup.xy by computing X.sup.y instep 116. Similarly, since Y=g.sup.y was transmitted from B to A in step 112, A can calculate the shared secret g.sup.xy by computing Y.sup.x in step 114.* The shared secret S can now be used by A and B as a session key for secure communication." (emphasis added)

Chen in col. 4, lines 32-56, shown below, teaches the use of private key and a public key for authentication, which teaches away from "*the subscriber station generating a random number and precomputing a first predetermined value when the subscriber station does not exchange a key for authentication with the authentication server*", as recited in claim 1 and similarly in claims 8, 15, 18 and 20. (emphasis added)

"Each authorized authentication server is assigned a private key and a corresponding public key by the token issuer or by a certification authority/key management agency 35. In addition, each token includes an embedded public key corresponding to a private key held only by the token issuer or certification authority, and not by the authentication server, and which allows the authentication token to verify the authenticity of the authentication server's public key.

The preferred procedure for implementing the invention thus *begins with the distribution of a token having embedded therein a public key Pi of the token issuer or certification authority (step 60)*, and at some time before or after distribution of the token to the user, *transfer to the server of the server's private key Pr* and signed certificates containing the server's public key Pu (step 70). Once the user has installed the token, the user is prompted to place a call over the open network to a chosen authentication server (step 80) which in turn transmits a signed certificate and registration template to the client application for verification based on the embedded public key Pi (step 90). If the user cannot verify the authenticity of the certificate because the certificate was not signed using a private key corresponding to the embedded public key Pi, or because the embedded public key Pi does not correspond to the private key used to sign the certificate, then the communication is terminated." (emphasis added)

Thus, Applicant submits that claim 1, and similarly claims 8, 15, 18 and 20, are not obvious in view of Halasz, MacKensie and Chen either taken singly or in combination, and are patentable over Halasz, Mackensie and Chen.

.

Should the Examiner disagree, Applicants respectfully request him to clearly and specifically point out where any of these references disclose or make obvious these features in accordance with 37 C.F.R. 1.104(c)2.

8. Dependent Claims

Claims 2-7, 9-14, 16-17, 19 and 21 depend on independent claims 1, 8, 15, 18 or 20. "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Therefore, in light of the above discussion, Applicants submit that these dependent claims are also allowable at least by virtue of their dependency on nonobvious claims as well as the additional limitations recited by each of these claims.

Conclusion

In view of the above, Applicants submit that the application is now in condition for allowance and respectfully urge the Examiner to pass this case to issue.

***

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 12-0415. In particular, if this response is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 12-0415.

I hereby certify that this document is being transmitted to the Patent and Trademark Office via electronic filing.

September 20, 2011
(Date of Transmission)

Lonnie Louie
(Name of Person Transmitting)

/Lonnie Louie/
(Signature)

/Lee W. Tower/
Lee W. Tower
Attorney for Applicants
Reg. No. 30,229
LADAS & PARRY LLP
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300